2001 TECHNOLOGY COLLECTION TRENDS IN THE U.S. DEFENSE INDUSTRY

Contents

This Defense Research and Technology Horizontal Protection publication was prepared by Mark Mooney, James Norvell, and Gene Smith. Comments and queries are welcome and may be directed to the DSS Counterintelligence Office at 1340 Braddock Place, Alexandria, VA 22314-1651. Special thanks to Emeric Butler for graphic design and lay-out and Laurie Dungan for editorial support.

Introduction

This fifth annual study is the Defense Security Service's (DSS) primary counterintelligence (CI) tool for security professionals. The data presented in this study is based solely on reports of suspicious foreign activity sent to DSS by Industrial Security Representatives and Special Agents. This information is based on information provided by cleared defense companies and cleared employees that experience foreign suspicious activity. DSS believes that this publication provides general information and conclusions that help cleared companies and DSS personnel recognize and report suspicious foreign activity so that DSS can assist cleared companies enact responsive, threat-appropriate, and cost-effective security countermeasures (SCM). DSS' proactive provision of relevant threat information for cleared contractors should further sensitize them to deter and detect suspicious foreign activity. Numerous government agencies also use this summary of reported information to analytically confirm or deny assessments of technology targets, to identify suspicious foreign actors, and to strengthen and supplement their investigative missions.

Key Judgments

Countries conducting conventional and nuclear arms races will seek U.S. defense contractors' weapons, sensors and countermeasures to obtain an advantage. Other foreign technology collection efforts will continue to address force modernization, economic competition, and commercial modernization, and will frequently target technologies with dual-use applications.

Foreign collection activities will continue to use automated systems to generate e-mail requests, solicitations, and website promoted inquiries. Suspicious Internet contacts will continue while use of the postal system and facsimiles will continue to decrease. Entities in developing countries will continue to mail inquiries and solicitations with postage.

Foreign entities exhibit frustration when effective SCM deny them sought information. In 2000, some companies denied and ignored requests similar to those foreigners made in 1999, which surfaced at other companies involved in similar research, technology and products. Due to the increased denial and non-response by cleared defense industry to foreign requests for information, foreigners will employ other collection methods and target different cleared facilities. This highlights the importance of reporting suspicious activity across the nation and overseas. Otherwise, DSS cannot monitor foreign entities, provide warnings, and detect and neutralize foreign threats.

Foreign suspicious activities that were predicated by or occurred in the conduct of a Foreign Military Sale (sometimes U.S. funded) will continue and may increase in 2001.

The increase in foreign targeting of machinery and fabrication technologies noted in 2000 will continue, perhaps increasing in 2001. Many protection discussions have addressed the economic threat posed by foreigners "reverse engineering" U.S. military products and acquiring manufacturing technology. (Although acquisition of manufacturing machinery is a threat, the greater threat is associated with countries acquiring other fabrication technology and production processes.)

Global business environments will continue to provide some degree of cover for foreign government-sponsored targeting of specific tech-

nologies and these suspicious incidents at U.S. cleared facilities are assessed to increase in 2001.

Executive Summary

Country Trends: In 2000, DSS received reports of suspicious activities concerning interests associated with 63 countries. The number of countries associated with targeting cleared defense contractors has increased since the start of this report. In 1997, 37 countries were linked to suspicious activity as compared with 47 in 1998 and 56 in 1999. DSS associates this increase with increased threat awareness by DSS field personnel and cleared defense contractors. These reports indicate that the majority of countries targeting cleared industry have limited advanced military capabilities (v. none) and are seeking technological advancement. In some instances countries possess older models and are attempting to upgrade specific sub-systems on a given platform.

Technology Interest Trends: The extent of foreign interest and collection methodology employed against specific technologies varies dramatically, from a passive request to sophisticated collection activities using various Methods of Operation (MO). The majority of targeted technologies, as well as those associated with Department of Defense (DoD) programs and weapons systems, was covered by the International Traffic of Arms Regulations (ITAR). As noted in 1998, foreign entities continue targeting weapon components, developing technology, and technical information more intensely than complete weapons systems and military equipment. For the first time in five years, suspicious activity reports concerning critical technologies do not include every militarily critical technology category. Foreigners targeted sixteen technology categories for military and/or economic exploitation. Directed Energy Systems and Weapons Effects systems received no reporting from cleared DoD contractors in 2000.

Most Frequently Reported Technology Targets: Technologies generating most foreign interest in 2000 included information systems, sensors and lasers, aeronautics systems, armaments and energetic materials, and electronics; in that order of frequency.

Most Frequently Reported Foreign Collection Methods of Operation (MO): MOs are the techniques employed by a foreign entity to collect intelligence or scientific and technical information against a given target. MOs associated with potential collection efforts in 2000 are as follows, ranked in order of frequency of occurrence:

- Request for Scientific and Technological (S&T) information.
- Soliciting and marketing of services.
- Acquisition of U.S. technology/company.
- Inappropriate conduct during foreign visits.
- International conventions, seminars, and exhibits.
- Exploitation of Internet (hacking).
- Exploitation of joint venture/research.

Unsolicited requests for information was the most frequently used collection method employed by foreign interests in 2000. While foreign interests employed a variety of methods, the methods are consistently similar to those reported during 1995-1999. Foreign collection methods and their frequencies are described in page 15. Enclosed Appendix identifies suspicious indicators and SCM that may mitigate the potential threats associated with these MOs.

Reporting

DoD Directive 5240.2 requires DSS to assist industry in recognizing and reporting suspicious activity. Cleared companies and DSS responded well in 2000, as in previous years. This active response continues a trend of increased awareness and reporting. The following criteria is used in assessing potential foreign collection efforts:

- Technology is classified/export-controlled.
- Information has national defense/military application.
- Redundant requests from same country for each technology target.
- Identifying consistent patterns across government agencies reporting on collection efforts by that country.
- Foreign entity is affiliated with foreign government defense organization.
- Request/offer is from an embargoed country.
- Possible front company and know technology target.

All threat information is evaluated in the context in which it takes place. DSS CI evaluates the military criticality of the requested information, whether it exists at the cleared defense contractor facility, association of the foreign collection method to those reportedly used by foreign intelligence services, history of suspicious activity by the foreign entity, and access of the contacted, cleared employee to the requested information. Only then can DSS CI apply a value to the threat information and then more rigorously analyze the information, if warranted. Foreign targeting, of interest to DSS, includes any classified technology, technology requiring an export license, technology listed in the International Traffic in Arms Regulation (ITAR) or Military Critical Technology List (MCTL). *(Only 2% of technologies targeted included recognizable classified technologies. As this is the first year identifying the classification of a technology. DSS assesses that there will probably be an increase in detection of targeting classified aspects next year.)*

MOs of interest to DSS include economic and industrial espionage activities related to an intelligence, scientific or technical collection operation. These activities normally involve a complimentary set of actions that vary based on a nation's culture, political system, business practices, and resources. These MOs include but are not limited to the following: request for information, violation of foreign visit protocol, exploitation of joint ventures, acquisition of U.S. companies or technologies, hacking, targeting cultural commonalties, targeting at international conventions, solicitation and marketing of services, exploitation of foreign employees, foreign collection against U.S. travelers abroad, and targeting former employees.

Submitted incident reports continue to emphasize the importance of using company Facility Security Officers (FSOs) as the central coordination point for each cleared company and each cleared employee. FSOs ensure timely and comprehensive review, of reported incidents, recognition of suspicious indicators, and reporting of suspicious activity. Special agents and industrial security representatives are encouraged and reminded to coordinate certain security activities among themselves when appropriate. Sometimes including the FSO in these discussions can be a security force multiplier.

Whether for investigation or analysis, reporting helps educate industry, security, and CI professionals about foreign collection methods employed against U.S. industry. Thus, to

provide thorough research and response, DSS Industrial Security Representatives refer to 12 information requirments listed in DSS ISOM section 1-5-302. Because the DSS CI Office needs to know some information in the greatest detail possible, the FSO may be able to help identify:

- The ultimate target (understandable description of technology, system, or research).
- Foreign identity (name, affiliation, descriptive features, previous contact, and postal and electronic addresses).
- Circumstances of the incident and background information (e.g., "met at convention in 1998," "denied a visit in 1999," "prime ignored several requests before foreigner approached us [subcontractor]").
- Suspicious activity (e.g., called a few times and e-mailed inquiring about program or technology)

Timely reporting of suspicious foreign activity enables DSS to evaluate foreign collection activity immediately, recommend threat-appropriate SCM, and expedite referrals to U.S. government agencies that can neutralize and exploit foreign efforts.

DSS has successfully contributed to government intelligence and law enforcement activities that resulted in the neutralization of foreign threats. In 2000, local referrals of exploitable information to government law enforcement activities increased as did resultant intragovernmental success in neutralizing threats.

Cleared company reporting also indicates numerous successes in applying appropriate SCM to potentially threatening situations. Based on information provided to DSS, cleared companies refused tours to unauthorized visitors, did not respond to suspicious foreign requests for information, asked for (and received) additional information from foreign entities, refused inappropriate visit sponsorship requests, used effective escorts to control visiting delegations, and questioned foreign entities about the reason(s) for their inquiries. This professional handling of foreign requests proved useful in identifying and reporting inappropriate foreign interests.

Most successes closely align with SCM outlined in the DSS brochure, "Suspicious Indicators and Security Countermeasures for Foreign Collection Activities Directed Against the U.S. Defense Industry." See Appendix for updated version. The expansion of indicators in this update indicates DSS and cleared defense industry security awareness training has been effective.

Country Section

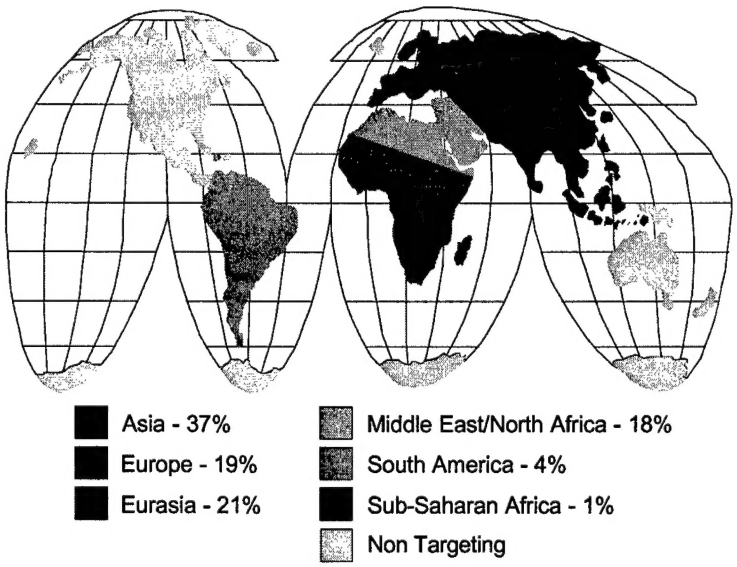
Since 1997, the number of countries associated with suspicious activities has continued to increase. The number of countries that are suspected of targeting U.S. critical technology is not entirely synonymous to those identified in cleared contractor reporting to DSS in 2000. Many countries exhibit interest in the same technologies. Newly identified countries, for the most part, were developing nations which may be interested in upgrading existing defense systems or developing a countermeasure that yields a battlespace or warning advantage. It is possible that some of the newly identified countries were collecting for other nations, whose own collection efforts have failed or need to be supplemented.

Table 1

Year	1996	1997	1998	1999	2000
# of countries with identified collection involvement	44	37	47	56	63

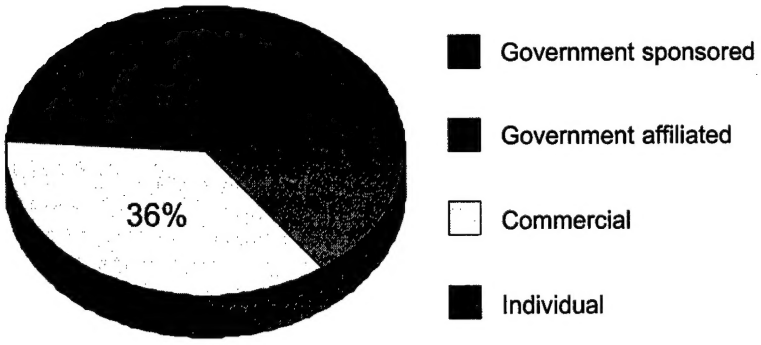
Figure 1

Worldwide Targeting Efforts



The map above denotes regions of the world from where collection efforts reportedly originated. The percentages indicate the level of collection activity reported in 2000. The map does not imply national level support of the collection activity. The collector may have based their operation in a third country to conceal intentions such as the ultimate end-user of the research or technology.

Figure 2



Technology

DSS documents and reviews foreign interest in critical U.S. defense technology in 18 categories. The Militarily Critical Technology List (MCTL) is the primary reference for DSS to identify and describe militarily critical technologies and sub-categories. The MCTL, especially Volume III, is a detailed and structured compendium of the emerging technologies the DoD assessed to be critical to maintaining superior United States military capabilities. The MCTL can be found on the Internet at www.dtic.mil/mctl. DSS employees should reference these volumes to identify technical or operational significance when addressing a suspicious incident.

A review of suspected targeting incidents in 2000 has found, for the first time in five years, that only 16 of 18 categories of critical technology were reportedly subjects of foreign interest for military and economic exploitation. Reports from all previous years involved at least one report relevant to each of the MCTL categories. Directed Energy Systems and Weapons Effects systems received no reporting from cleared DoD contractors in 2000. The extent of foreign interest in the remaining technology categories varies dramatically. In some cases, nations were associated with targeting all technology categories while others were only associated with targeting a single technology.

Information Systems (IS) was the most widely sought militarily critical technology category in 2000, as it was in 1999. IS showed the greatest targeting interest with 33 of the 63 countries associated with suspicious collection activity. Sensors and Lasers was the second most targeted technology with 24 countries involved in collection efforts. Tied for third most widely sought technology was Marine Systems and Armament & Energetic Materials technology. Seventeen countries were associated with collection efforts targeting each of these. The statistics discussed in this section are based solely on those technologies identified in suspicious activity reporting from cleared contractors.

Because of varied technology applications and the wide range of military and economic for-

Table 2

Technology Interest Trends

Military Critical Technology List	Percentage Targeted
Information systems	30%
Sensors and lasers	17%
Aeronautics	9%
Armaments and energetic materials	8%
Electronics	8%
Marine systems	6%
Chemical/biological systems	3%
Manufacturing and fabrication	3%
Signature control	2.5%
Guidance/navigation/vehicle	2.5%
Space systems	2.5%
Materials	2%
Nuclear systems technology	1.5%
Ground systems	1.5%
Information warfare	.5%
Power systems	.5%

eign interests, cleared contractors are encouraged to provide additional application details. Identification of how the foreigner intends to use the U.S. technology, such as military acquisition, helps DSS analysts determine foreign trends, intentions, actual targets, planned usage, and the program or upgrade with which the technology is, or may be, associated.

DSS believes that when we identify all specific technologies that have been targeted by foreign interests, this increases the threat awareness of cleared companies, DSS agents, and industrial security representatives. On the following pages, these specific technologies are indentified in each militarily critical technology category. DSS hopes that this increased awareness will promote relevant security considerations and additional reporting of suspicious incidents that may not have been previously noticed. Because many cleared companies are involved with many technology areas, DSS values identifying the percentages of foreign technology targeting efforts. This information may assist cleared companies to compare and contrast relevant threat data and decide upon threat-appropriate security measures and countermeasures.

The majority of defense technologies targeted in 2000 was components vice complete systems. This trend has continued to increase since 1998 when DSS first noticed developed and developing countries were upgrading existing platforms. Most frequently reported technology targets by MCTL Category and volume of reports were:

Information Systems remained the most sought militarily critical technology category in 2000. IS showed the greatest diverse interest from 33 of the 63 countries associated with suspicious activity. IS are pervasive in virtually all military, commercial and industrial activities, and all levels of government. This may explain the 100+% increase in reported Information Security targeting over 1999 reporting. The greatest increases in foreign targeting occurred in information security, transmission systems, and software systems sub-categories.

Information Security technologies are vital to U.S. warfighter capabilities. Uses of IS encompass a wide range of applications from IS embedded in individual smart weapons and sensors, to local processing and communications systems, including transportable and personal hand-held devices, to international wide area computer networks. Access to these technologies by potential adversaries could enhance the performance of foreign military systems and could be used to counter U.S. capabilities.

Significant foreign interest in 2000 included: modeling and simulation technology (military training systems), C4I such as: HF, VHF military radios, and INFOSEC encryption devices (KG-194, KG-84 a/c, KIV-7HS, KG-81, KG-94), TEMPEST equipment, firewall and intrusion detection technology. Other reports concerned SATCOM systems and signal processing components.

Table 3

Collection Incidents per Sub-category per Year

Information Systems	1996	1997	1998	1999	2000
Command, Control Communications, Computing, Intelligence (C4I)	4	6	5	5	8
Computer Aided Design, (CAD) Computer Aided Manufacturing (CAM)	0	1	1	2	4
High-Performance Computing	5	2	5	0	3
Information Security	7	13	6	2	21
Intelligence Systems	8	4	3	0	11
Modeling and Simulation	5	5	6	6	12
Network Switching	0	4	1	0	1
Signal Processing	2	0	1	3	9
Software Systems	5	10	15	13	33
Transmission Systems	21	5	6	4	29

Transmission systems saw the greatest increase in targeting in 2000. Transmission systems include equipment and components used for transfer of voice, data, record and other information by electromagnetic means; through atmospheric, exoatmospheric, or subsurface media or via metallic or fiber-optic cable. The information being exchanged is predominantly in digital form of voice, text, graphics, video and databases.

Significant interest in acquiring communications security devices was noted due to good reporting in 2000. Several DoD contractors received requests to purchase encryption devices, one incorporating Firefly technology and the other used for digital and voice bulk encryption. Other reports indicated foreign interest in the "VINSON communications security equipment" and another military communications security product.

Sensors and Lasers remained the second most frequently targeted defense technology reported by cleared contractors and foreign targeting increased by 2 percent. There were 24 nations associated with targeting sensor and laser technologies. Five countries accounted for 63 percent of these incident reports. Those countries with superior sensors have a significant advantage over an adversary. Arms races are excellent examples of why countries seek early warning advantages, hence advanced sensors, to monitor neighbors and regional threats. Though targeted sensors were greatly varied systems with diverse functions, their commonality is that U.S. state-of-the-art sensors are generally better than the rest of the world.

Targeting in the electro-optical field tripled. Electro-optical sensors are typically used for night vision devices and for terminal guidance for smart weapons. This equipment ranges from night vision goggles for individual personnel to large telescopes, vehicle driver systems and weapons sights. The majority of sensor targets in 2000 involved night vision . These critical systems depend on second and third generation image intensifier technology; micro-channel plate amplifiers and compounds, semiconductors, and photo-cathode tubes.

In one 2000 case, military representatives continually requested third generation imaging technology. Some countries define third-generation systems as those using large two-dimensional staring Focal Plane Arrays (FPAs). At least one foreign firm currently markets its staring system under a third generation label because it uses a 320X240 InSb FPA. In the U.S., the definition of third-generation systems is still being formed. Third generation systems are often reserved for aviators or tank drivers who are moving at fast speeds and need to process information quickly. If exported, tankers and pilots would most likely use requested night vision devices militarily. Normally, ground units receive second generation devices. In this country, night vision devices observed being utilized by foreign military personnel were in poor condition, NOT operationally ready. DSS notes that dire needs contribute to foreign technology collection activity.

Other targeted technologies included underwater acoustics, infrared (IR) detectors, airborne and ground radar, imagery dissemination software, digital terrain data, IR imagery, optical night vision products, photonics, thermal imaging camera, antisubmarine warfare (ASW) acoustic detection systems, electro-optic sensors, passive communications intercept and electronic intercept receivers. Laser technologies targeted in 2000 included radars, range finders, pulsed lasers and U.S. designs. Note comparisons to previous years.

The "other" sensor category currently pertains to passive communications and electronic intelligence receivers for land, air, and sea employment and other detection and surveillance devices not affiliated with specified categories.

Table 4

Collection Incidents per Sub-category per Year

Sensors and Laser Technology	1996	1997	1998	1999	2000
Acoustic	2	4	18	2	5
Electro-Optical Sensors	6	3	13	3	9
Focal Plan Array/Infrared	1	8	11	5	5
Radars	10	5	8	22	9
Imagery	6	5	13	8	3
Lasers	0	0	0	4	8
Other	6	2	10	5	14

Aeronautics Systems was the third most frequent technology target while foreign targeting efforts directed against it remained at 9 percent of total reporting. Identified 2000 targets included: EA-6B, F-15, U.S. CH-47, F-22 aircraft, Unmanned Aerial Vehicles (UAVs), and ALQ-144 airborne infrared countermeasures set for helicopter survivability.

There were 15 countries associated with suspicious activity directed against aeronautic technologies. One country accounted for 4 of 23 targeting efforts associated with aeronautics systems followed by another country's interest (3 collection attempts) targeting components of U.S. special electronic mission aircraft.

Incident: a foreign firm recently requested UAVs from a cleared DoD contractor for an unspecified foreign client (third country) that was believed to be embargoed. The two countries, requestor and client, have been negotiating the upgrade of an embargoed nation's UAV. The embargoed nation's UAV research and development activity has been minimal to non-existent since the mid-1980s due to embargo constraints, poor maintenance, a lack of skilled operators and limited funding. In the past ten years, two countries have offered the embargoed nation advanced UAV technology upgrades to include composite aircraft materials, equipment and technical assistance. The embargoed nation also sought upgrades for the UAV program from a number of nations. The embargoed nation's UAV program may continue and may become more of a threat to regional U.S. interests and U.S. forces.

UAVs have made greater strides over the past 18 months, in terms of widespread acceptance by the user community. Unmanned systems are now beginning to be seen as cost-effective and advanced-technology alternatives to manned platforms. Several factors have contributed to this rapid development. UAVs were employed by at least five NATO member countries during last year's Operation Allied Force over Kosovo. This provided valuable experience and taught several important lessons. UAVs confirmed their value to the warfighter for intelligence, surveillance and reconnaissance, and combat support applications. They also demonstrated the flexibility required for rapid changes "on the fly" to meet emerging needs beyond their traditional role, such as working with airborne forward air controllers in F-16s. This information is provided to explain why foreigners who were initially interested in manned aircraft may become interested in UAVs. This change of interest, per se, is not cause for concern. Export controls should regulate foreign acquisition attempts.

Several suspicious incidents occurred during approved foreign military sales. A foreign aviator wanted to know the difference between the U.S. F-15 and the export model his government received. On five separate occasions foreign Air Force officers approached cleared DoD contractors requesting information regarding the differences between the U.S. F/A-18D and the version their country received as well as the versions that the U.S. provided to Spain and Singapore. Additional questions concerned various equipment associated with the F/A-18D including AN/ALQ-126 processor, AN/ALE-47 countermeasures dispenser system, and the AN/ALR-67 (V) advanced special receiver.

Table 5

Collection Incidents per Sub-category per Year

Aeronautics	1996	1997	1998	1999	2000
Aircraft, fixed wing	5	10	5	6	11
Gas turbine engines	4	8	5	7	3
Human (crew systems) interface	6	1	5	0	1
Helicopters	2	3	1	1	4
Unmanned aerial vehicles	2	4	4	1	4

Armaments and Energetic Materials include those required to develop and produce in quantity safe, affordable, storable, and effective conventional munitions and weapons systems of superior operating capability. These include infantry and crew serve weapons systems, ammunition, artillery weapons systems, torpedoes, depth charges, bombs, land and sea mines, demolition devices, high explosives, kinetic energy and pyrotechnic warheads, projectiles, sub-munitions, fuses, safety and arming devices and other components.

Technologies targeted in 2000 include TOW missile, R-77 medium range missile, flame spray gun, large caliber ammunition, fuse technologies, cruse missile technology, sidewinder AIM-9P missile, Mark-45, and PAC 3 including classified performance characteristics and safety systems. Five countries were associated with the vast majority of targeting.

Table 6

Collection Incidents per Sub-category per Year

Armaments & Energetic Materials	1996	1997	1998	1999	2000
Ammunition, small/medium caliber	0	0	0	0	0
Bombs, warheads, large caliber projectiles	1	5	8	4	16
Energetic material	0	0	1	1	1
Safing arming, fusing, firing	0	1	1	0	5
Gun and artillery systems	0	1	4	4	1
Mines, countermines and demolition systems	0	1	1	0	1

Electronics Foreign targeting of electronics technologies decreased 2 percent to 8 percent in 2000, moving it from third to fifth place. The majority of targets concerned defense applications of dual-use electronics such as microwave components, wafer fabrication, silicon photodiodes, high voltage systems for night vision goggles, tank sites, rifle scopes, and tempest/hardening of equipment.

An embargoed nation led foreign entities targeting electronic technologies, accounting for 23% of reports. Three other countries accounted for 10% each of reports concerning this technology. Due to the nature of reported incidents it is clear foreigners were interested in military applicable electronics, although only 9 fit neatly into sub-categories.

Table 7

Collection Incidents per Sub-category per Year

Electronics	1996	1997	1998	1999	2000
Materials/components	2	4	6	12	1
Fabricated materials	1	2	3	1	0
Microelectronics	5	5	2	4	7
*Optoelectronics	1	4	1	3	1

*Many optoelectronic targets in 1997 may have concerned sensors. Detailed 1998-2000 reporting helped DSS identify optoelectronic targets that were being applied to sensors.

Marine Systems remained (and now tied) in fifth place accounting for 6 percent of foreign targeting. However, actual incidents declined by 3 percent. Specific technologies targeted included submarine propulsion systems, ship and submarine construction, swimmer delivery vehicle (restricted version), underwater tracking systems, amphibious assault ships, submarine masts, and driver propulsion vehicles. Several targeting efforts involved the Navy's DD-21 Program. Foreign interest in U.S. antisubmarine warfare continued at the same level as 1999. Several foreign contacts concerned marine systems but not specifically these sub-categories. Other targets included aircraft carrier and runway specifications, port data, and ship building techniques.

Table 8

Collection Incidents per Sub-category per Year

Marine Systems	1996	1997	1998	1999	2000
Propulsors and propulsion systems	N/A	3	1	0	1
Signature control and survivability	N/A	1	2	2	5
Subsurface and deep submergence vehicles	N/A	2	0	2	3

N/A means that no reports indicated these specific technologies were targeted. Other marine systems such as engines were targeted in 1996.

Chemical/Biological Systems targeting increased by 1 percent to more than 3 percent, moving it from fourteenth to sixth place. Chemical and biological systems address bio-processing, chemical manufacturing; chemical and biological defense systems; chemical and biological detection, warning, and identification; battlefield environment; and human factors. The majority of foreign requests in this category were for published research.

Manufacturing and Fabrication Collection efforts directed at manufacturing and fabrication technologies also increased by 1 percent to nearly 3 percent, moving it up to seventh place. Technologies covered under manufacturing and fabrication include those required for the production of military hardware. In most cases the technologies, the equipment and the know-how are dual use. All countries engaged in the production of military weapons, munitions, and systems possess, to some degree, technical know-how in this area. Frequently U.S. techniques rather than equipment are targeted by foreign entities.

Signature Control Signature control technology is critical to certain U.S. weapons systems because it reduces an adversary's ability to detect, track, monitor and engage during combat operations. This technology may increase the ability of the U.S. to detect foreign weapon systems that have low observable features. Targeting associated in this area decreased by 1 percent to just under 3 percent. One key area of foreign interest (particularly for one country) was stealth associated with anti-submarine warfare.

Power Systems Electric power drives subsystems and systems in hundreds of U.S. military platforms and end-items. These various applications dictate military requirements for power level, power reliability, ruggedness, packaging and ability to operate in a variety of environments. Foreigners targeted pulsed power generators and flat cell technology.

Guidance, Navigation and Vehicle Control Targeting associated with guidance, navigation and vehicle control decreased 2.5 percent in 2000, moving it from seventh to ninth place. Specific targeted technologies included global positioning system (GPS) and gyroscopes.

Space Systems Space and space technologies are vital for the military, defense, and economic security of the United States. Space technologies include platform electronics and computers, optronics, power and thermal management, propulsion systems for space systems, and sensors for space systems. Technologies targeted in 2000 included software associated with satellite operations, satellite brackets, and sensors and electronic modules.

One suspicious incident involved a foreign engineer from an embargoed "Research Organization for Science and Technology's Mechanical Engineering Department" requesting hardware equipment for small satellites. He stated that he was building a satellite for the purpose of conducting research. However, satellites are usually operational before they can conduct research.

Materials Many classes of materials inherently have both military and commercial application. Critical materials provide specific military advantages and cover the physical properties, mechanical properties, behavior, and processing required to achieve that advantage. Technologies targeted in 2000 included abrasive media, casting processes, high module carbon fibers, and ceramic technologies.

Nuclear Power Systems critical components include technologies for processing man-made fissile materials, for processing and handling highly radioactive and corrosive materials, for producing plutonium and tritium reactors, and for producing and assembling nuclear weapons components. Targets in 2000 included ion-implanted/surface barrier, fabrication and manufacturing techniques.

Ground Systems address technologies, excluding weapons systems, associated with combat vehicles that enable these systems to be superior to opposing systems in combat. Despite the high percentage of dual-use technologies applied to military air, ground and sea vehicles, unique physical and operational capabilities are often required. Targets in 2000 included robotic vehicles, tank systems fuel components and armored vehicle track designs.

Information Warfare is defined as actions taken to achieve information superiority by affecting adversary's information, information based processes, and computer based networks while defending one's own information. Technologies targeted in 2000 include pin diode switches (used in communication jammers), and command and control warfare technology.

Foreign Collection Methods of Operation

Statistical accuracy on foreign collection methods of operation (MO) has improved in 2000 due to more detailed reporting from cleared defense industry.

Table 9

Foreign Collection Modus Operandi	% Employed
Request for information	41%
Solicitation and marketing of services	18%
Acquisition of technology and companies	13%
Foreign visits to U.S. Facilitites	8%
International conventions/exhibits	4.5%
Internet activity (hacking)	4%
Exploitation of joint ventures	4%
*Foreign collection v. overseas travelers	4%
Targeting cultural commonalities	1%

*Foreign collection missions directed against U.S. persons traveling outside of the U.S.

Suspicious Foreign Requests for Information (RFI). Incidents involving RFI continue to be the most frequently reported MO; accounting for 41 percent of the total activity recorded in 2000. This represents a 4 percent decrease from 1999. Included in this category is any request not sought, or encouraged by the cleared company, which is received from a known or unknown source (usually foreign), which concerns classified, sensitive, or export controlled information. The information targeted in 2000 included classified, sensitive but unclassified (which frequently is company proprietary products, information, software and processes), and export-controlled information. Requests originated from foreign government organizations, government-sponsored or affiliated organizations (laboratories and institutes), foreign commercial activities, and foreign individuals. While the recipient may not directly solicit the request, the inquiry may actually have been indirectly solicited. An example of an unwanted, but indirectly solicited request is an incident where a cleared defense contractor's product was reviewed in a trade journal and the company subsequently received a number of suspicious, but "solicited," reader-service card inquiries from an embargoed country.

Between 1998 and 2000, DSS saw an increase in the reporting of requests for information from countries that do not normally conduct business with the U.S. such as embargoed countries. These requests accounted for 50% of all foreign attempts to collect International Traffic in Arms Regulated (ITAR) information and technology. A commonality in the vast majority of these suspicious contacts, was that the request was for informational exchanges requiring an export license in accordance with the ITAR. RFI received from countries with highly restrictive political, social and business environments still favor the use of the postal system. This does not imply that only embargoed or restricted countries rely on traditional written correspondence. In fact, ironically, the majority of suspicious letters originated from countries with developed electronic connectivity to the U.S.

From 1997 to 1999, DSS reported an increase in the use of the "thesis or scholarly request" strategy. This trend remained constant in 2000 reporting. The thesis request usually targets a specific individual at a cleared facility. The "student" will state he/she is working on a thesis, likely in a field indirectly related to a protected U.S. technology. The student then states that he/she located the U.S. employee's name while conducting initial research. The student will ask for whatever assistance the cleared employee can provide, including articles. The information requested, including copies of technical articles, might provide new information confirming existing assumptions about U.S. technology and serve as a means to identify targets for exploitation.

One such student from Europe requested "integrated logistics support" software technology, which just happened to be classified information. The cleared facility was working on technical and specialty engineering programs at the time. Another frequently used tactic is the "model builder". The model builder asks for specifications, which most likely would not affect the design of any model such as cockpit or turbine engine specifications.

An increasing trend observed in 1999 and again in 2000 concerns suspicious requests from foreign universities and research institutes. A majority of these entities are state funded and are heavily involved in military applicable technologies. Representatives of the research centers attempt to collect information on foreign technology through the use of technology exchanges and discussions with

experts. These collection operations involve identifying and contacting experts in various fields of interest and forming greater cooperation with U.S. defense contractors and military Research, Development, Test, and Engineering (RDT&E) facilities. Some e-mails of this type were received by cleared employees and foreigners' e-mail addresses could in no way be associated with the institute or university. One used hotmail and maintained anonymity until the cleared employee inquired, "Who do you work for and what will you use this [technology] for?" Often at this point, as in this case, foreigners provide enough details for the company to know whether to proceed with discussions. Cleared companies have expedited this type of information to DSS several times which led to a number of arrests by other U.S. government agencies.

Since 1998, the Internet continues to be a significant source of foreign collection of U.S. DoD technologies. The use of the Internet as a collection tool used by foreign entities to collect U.S. technology and technical information accounted for 27 % of all suspicious contact reports made to the DSS by cleared defense industry. This percentage reflects the growing role of the Internet in conducting business. A wealth of once protected technical and proprietary information is now easily retrievable by individuals from around the world. For example, a cleared defense contractor was surprised when he received an e-mailed RFI regarding his company's mapping software from an embargoed foreign company. The contractor's e-mail address was listed as a point of contact on the small company's web site which also highlighted the company's technological advances in mapping software.

There continues to be a sharp increase in the use of the Internet by foreign entities as a tool to identify potential targets and to facilitate the actual collection of information. The Internet provides a simple, low-cost, non-threatening, risk-free means of worldwide access to U.S. defense technology. E-mail and WEB-chat exchanges are inconspicuous and can bypass many traditional security safeguards, directly reaching the targeted individual. Requests over the Internet continue to account for almost half of the total Internet reporting. Cleared contractors who most often report Internet based requests have active monitoring solutions in place to protect their unclassified web sites. These contractors regularly incorporate security with their web site design and advertising.

DSS attempts to determine whether cleared defense web-based advertising predicates foreign suspicious requests. When a suspicious report is made to DSS, our industrial security representatives and special agents ask the cleared defense company if they believe their web-based advertising caused the foreign contact or request and why they think the request is suspicious. Indicators that make requests suspicious are: the cleared defense company does not normally conduct business with the foreign sender, the request originates from an embargoed country, the request is in fact unsolicited or unwarranted, it appears the requestor is utilizing a third country return address, the requestor makes claims he/she is representing an official government agency but has gone outside of channels to make the request, the initial request is directed at an employee who does not know the sender and is not in the sales or marketing office, the sender appears to be fishing for information, the requestor represents a third party who is not identified, the requestor is located in a country with a targeting history directed at

U.S. cleared defense industry, or the sender appears to be avoiding controls or circumventing established procedures, such as avoiding export license application.

In many circumstances, when foreign individuals attempt to skirt controls, they will mask their true intentions and e-mail several similar requests for information. These requests are usually innocuous and not threatening. The reason for this is foreigners are trying to mask their collection activity. Their goal is to establish credibility in order to obtain more sensitive and sometime classified information. For example, over a period of ten days a U.S. cleared defense company received three foreign e-mailed requests asking the company to provide its software development product to the foreign sender. The foreign sender was the same in each case but the sender used multiple e-mail addresses.

Foreign scientists and engineers have initiated contact with U.S. companies/employees from each type of establishment listed below.

Table 10

Institute/University
Aircraft Design & Research Institute
Federal University
Technical Institute
Academic University
Institute of Chemical Physics
University of Science and Technology
Institute of Physics
Institute of Nuclear Technology
Polytechnic University
Research Institute
Institutes of Advanced Electrical and Electronic Engineering
Institute of Aircraft Maintenance
University Physics Department
Electrotechnology Research Institute
Military University
Technical University
Institute of Semiconductor Physics

Solicitation and Marketing of Foreign Services moved into second place on our list of most frequently used foreign collection methods. Solicitation and marketing of services was the third most frequently reported in 1999, moving up from fourth place in 1998. Consistent with past reporting; individuals, companies and research facilities offer their technical and business services to U.S. research facilities, academic institutions and the cleared defense industry in 2000. These foreign entities also ask to represent the cleared company's product line in their country or regional area. As in 1999, many of these solicitations concerned provision of foreign software services.

One very popular approach to cleared defense industry is the "foreign scientist" seeking employment. Companies receiving such solicitations for jobs include facilities working on: nuclear engineering, electro-optics, ballistics, astrophysics, and materials. Other approaches include software support, internships, invitation to ambassadorial programs and offers to act as sales or purchasing agent. Of growing concern is the use of foreign research facilities and software development companies located outside the U.S. working on commercial projects related to protected programs. Anytime a U.S. cleared facility relinquishes direct control of its processes or product to someone else, they are exposing technology to possible exploitation.

In July 2000, a U.S. cleared defense contractor decided to purchase a phone system and solicited bids including foreign bids. Due to prior training and liaison conducted between the company's FSO and DSS' Industrial Security Representative, the U.S. company requested threat information concerning foreign bidders. Working with his DSS Field CI Specialist both realized immediately the threat to the U.S. entity. The U.S. entity, among other things, works on a contract for the Marine Corps related to its theater level ballistic missiles. Based on the information provided by the U.S. entity, the leading foreign bid came from a foreign entity which accounted for at least four suspicious contact reports submitted by cleared defense industry to DSS-CI. In each report the same technology was targeted at U.S. cleared defense facilities -- information systems. Also, the leading foreign bidder was the subject of many reports within the intelligence community. Both DSS employees, relying on historical knowledge of the U.S. entity and the foreign threat to U.S. cleared facility, provided a threat appropriate response to the U.S. entity. The response included a threat assessment produced by a U.S. military production center and directly addressed the threat inherent in the foreign bid to provide vendor services to the U.S. company. The document allowed the U.S. company to mitigate risks they did not want to incur while trying to protect classified and Marine Corps information by assessing risks posed by the leading foreign bid, or any foreign vendor. The U.S. company selected a U.S. contract at a higher cost. Ultimately, DSS saved a company's proprietary information and quite possibly Marine Corps technology from foreign exploitation.

Acquisition of Sensitive Defense Technology or Cleared Company Acquisition was the third most often used MO reported in 2000, up from fourth position in 1999. This is only the latest manifestation of an increasing trend to acquire sensitive technologies through purchase. Acquisition attempts accounted for 88 % of reported suspicious incidents believed to involve a third party. Third party involvement indicates possible technology transfer or diversion. Third parties are not the actual entity acquiring the technology but are the end user or ultimate recipient. Reports involving third parties include either a country with a history of third party sales or a country used by other, often embargoed, foreign countries as a venue for purchase and collection. Statistics show no clear distinction between U.S. defense technology requested for purchase by developed and developing countries.

Developing countries continue to consider, and seek purchase of, older U.S. military technologies for varied reasons: older technology may not require a license, older equipment may be best incorporated into existing logistics and maintenance systems, old technology best suits critical shortages for a country at war, or a country cannot incorporate and maintain new technology because its industrial base is inferior to U.S. level of technology sophistication. The purchase of U.S. products in small quantities may indicate reverse-engineering efforts that may help countries determine whether their industrial/manufacturing systems can produce domestic models/copies.

In 2000, sanctioned nations involved in border and landhold conflicts increased their attempts to acquire sensitive defense technologies, primarily sensors. Several resultant law enforcement actions were attributed to DSS reporting of these incidents.

The majority of foreign purchase attempts in 2000 concerned TEMPEST equipment and encryption devices including the KIV-7HS, which are export controlled. Other requests include a wide range of technologies and systems such as: HF ocean surface radar, strip detectors for x-ray radiation, long range laser finders, microwave control systems and acceleration sensors. Some technologies may be sought with the stated intent for civilian use such as infrared (IR) lenses, but may have applications in larger ITAR controlled systems including focal plane array technologies, which are used in sensors and laser guided munitions. Some defense articles require more than a general export license for sale to a foreign country. The uses of freight forwarders and "cooperative U.S. based companies" have been suggested by foreigners and may be employed because they give a foreign entity a U.S. address. The U.S. company is compromised because the final destination is not the U.S. but a location outside the U.S.

Exploitation of Visits to U.S. Companies Reports concerning suspected exploitation of foreign visits at U.S. facilities was fourth in frequency of reporting. The term "foreign visitor" includes one time visits, long term visitors (such as exchange employees, official government representatives and students) and/or frequent visitors (such as foreign sales representatives). Suspicious conduct includes actions before, during and after a visit. The one factor which made many foreign visits suspicious was the extent to which the foreign visitor requested access to facilities or tried to discuss information outside the scope of approved activities or established procedures.

In several incidents in 2000, foreign visitors ignored Technology Control Plans (TCPs). A TCP stipulates how a company will protect its technology. The plan establishes procedures to protect classified, proprietary, and export-controlled information, to control foreign visi-

tor access, and to control access by non-U.S. employees. In one example, a group of senior foreign executives arrived at a scheduled briefing in a cleared facility and made a formal request for the meeting to be held at another facility nearby. The nearby facility was the facility containing the classified project. Suspicious indicators associated with foreign exploitation of visits to U.S. facilities traditionally include:

- Behaving inappropriately during a visit: Wandering around the facility unescorted, bringing unauthorized cameras and/or recording devices into the cleared facility, or pressing for additional access or information and becoming irate upon denial. In one case, a foreign visitor excused himself from a conference stating he needed to get his briefcase in the sponsor's office. Later he was found in the sponsor's office speaking on a telephone in a foreign language. He quickly ended the conversation when approached.

- Adding last minute and/or unannounced persons as part of the group.

- Making numerous requests for visits, despite repeated denials.

- Brokering a visit. A brokered visit is when a third party, who is not involved in the actual business transactions, acts on behalf of the prospective visitor to arrange for an invitation to be extended to the foreigner. Brokered visits become suspicious when the third party bypasses established foreign visit request procedures by going directly to a company employee to solicit an invitation for the visit. Brokers often cloak their clients' employer until queried by the U.S. company.

- Arriving unannounced and seeking access by asking to see an employee who may belong to the same business organization or who had attended the same business gathering as the foreign national.

- Hiding true agenda such as trying to shift the conversation to topics not agreed upon.

- Misrepresenting a visitor's importance or technical competence to secure visit approval.

Targeting at Conventions moved up to fifth place in frequency of use by foreign entities. Conventions continue to provide a "target rich" environment for foreign intelligence collection as they directly link U.S. programs and technologies with knowledgeable personnel. International exhibits provide a unique opportunity for foreign entities to study, compare, and photograph actual products in one location. Some technologies targeted at conventions include laser optics, obscuration smoke systems, submarine and ASW specifications, PAC 3 safety systems, and air defense technologies.

International seminar audiences are often comprised of leading national scientists and technical experts, who pose more of an exploitation threat than intelligence officers because the scientist's/engineer's level of technical understanding and ability can readily exploit U.S. technology and information for their nation's advancement. Foreign technical experts focus questions and request specific technical data that directly applies to their work. Reports show that during seminars, foreign entities attempt subtle approaches such as sitting next to a potential target and initiating casual conversation. This can establish a point of contact that may later be sub-

jected to exploitation. Membership lists of international business and/or technical societies are increasingly used to identify potential U.S. targets for introduction. Because the threat is designed to exploit the cleared defense employee, the approach will most likely be very subtle and unrecognizable. Most likely, the targeting will be directed at U.S. persons with cultural commonalties such as origin of birth, religion or language.

Internet Activity (hacking)

Targeting associated with exploitation of the Internet (hacking) fell back to 6th place. *(NOTE: This category is not related to the Internet-based requests. Because DSS does not analyze or forensically investigate these incidents, our statistics may be limited to initiative reporting by companies not referring these matters to the FBI. When received, DSS forwards these reports, sometimes with analytical assessments or conclusions, to the FBI's National Infrastructure Protection Center.)*

The majority of foreign Internet activity was probing efforts. The computer probes are most likely searching for potential weaknesses in systems for exploitation. In one example, a network attack originated from Europe. The attack lasted over a period of a day. Several hundred attempts were made to use multiple passwords to illegally obtain access to a cleared facility's network. All attempts were logged by the firewall monitoring software and no malicious activity was encountered. The facility had the appropriate level of protection in place to repel such an attack. By detecting probes, the cleared companies demonstrated they have the SCM in place to thwart attempts to penetrate their computer systems. Although probing a system is legal, once a port is breached a crime is committed.

Exploitation of Joint Venture/Research dropped into a tie for 6th place in frequency of reporting. This MO offers significant collection opportunities for foreign interests, as well as venues for expanding their industrial base or production capability without having to pay for the research and development. Joint venture reporting may have dropped off due to reporting inconsistencies. For example, some facilities may have reported a foreign visit instead of the joint venture, which may have predicated the foreign visit. DSS tries to differentiate between joint ventures, which are also known as international programs and cooperative agreements, from non-associated visits. Cleared companies can help DSS recognize this difference by informing representatives during security discussions. As with frequent foreign visits and other international programs, joint ventures place foreign personnel in close proximity to U.S. personnel and technology and can facilitate access to protected programs. Also of concern is the placement of foreign workers in close proximity to protected operations. Once a foreign employee is in place for a long time, that foreign employee tends to assimilate into the standard workplace image, be more accepted and, therefore, security considerations become a lower priority.

Indicators of suspicious activity in a joint research/venture include: the foreign worker seeking access to areas and information outside the purview of the work agreement, enticing U.S. contractors to provide large quantities of technical data as part of the bidding process, and the foreign organization sending more foreign representatives than reasonably necessary for the project. Some targeting of joint ventures included advanced casting techniques, firewall and intrusion detection technology, laser head design (a patented melt-down manufacturing process), and simulator technology.

Foreign Targeting of U.S. Travelers Overseas DSS saw increased reporting of foreign collection activities directed against U.S. cleared employees on official or business travel. Increased reporting prompted DSS to categorize this foreign collection activity as a distinct foreign method for collecting U.S. technology from U.S. cleared defense employees. Suspicious incidents usually occurred during foreign travel on trains, at airports and in hotels. This category does not include incidents that occur at conventions, seminars, or exhibitions. This MO is in a three-way tie at sixth place for frequency of use by foreign entities. Events held on the collector's home territory leave U.S. business travelers vulnerable to exploitation by traditional Foreign Intelligence Services (FIS) technical means (for example, electronic surveillance) and the employment of entrapment ploys (such as inducement of the target into a compromising situation). Cleared defense contractors should review the type and amount of information contained in the registration, biographic and other materials requested by the host. A number of official events cause U.S. business travelers to be recognized by FIS including international conventions, combined military operations and joint ventures.

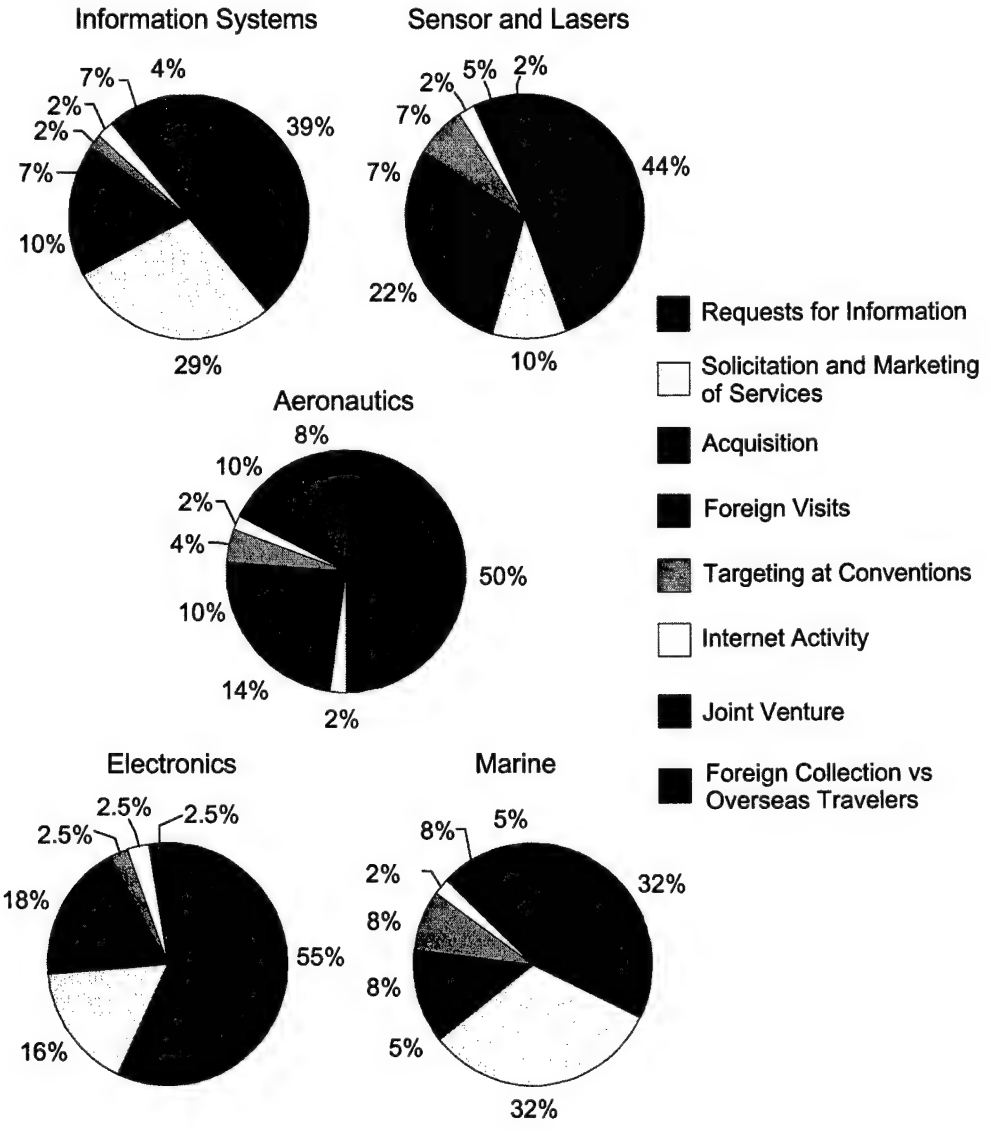
In one case, cleared contractor representatives staying at the same hotel reported several attempts to gain access to their rooms. In another incident, a defense contractor reported a family member went back to his hotel room after dinner to find an opened notebook computer in the middle of the bed. The computer had been stored with the luggage before dinner. Repeat U.S. visitors have been assigned to the same room over a long period. Other travelers received excessively "helpful" service by host government representatives and hotel staffs. The majority of suspicious activity during overseas travel is reported in relationship to a hotel stay.

In other cases, short-term custodial detentions by host government officials occurred at airports and waterways during which foreign officials attempted to gain information regarding the U.S. traveler's visit. The majority of airport detentions occurred at only one foreign airport.

Foreign Collection Methods by Technology

Technology/MO Correlation. As mentioned in the introduction, MOs used must be viewed in the context of the overall atmosphere of the collection operation. No one rule is applicable to all foreign collection attempts. The charts below display the prevalent MOs employed against the most sought after technologies.

Figure 3



Assessment of Future Trends

DSS forecasts that countries assessed as moderately and most active in 2000, will continue collection operations at similar levels against cleared U.S. defense industry in 2001.

DSS assesses that if cleared employees and cleared defense contractors do not respond to requests, foreign collection activities will employ additional MOs to include foreign visits and may also target other companies.

Based on 2000 reporting, DSS believes that targeting of cleared defense industry from foreign institutes, businesses and individuals (versus recognizable foreign government entities) will continue. Recognizable foreign government contact will decrease. DSS assesses that Foreign Intelligence and Security Services (FISS) will direct some of these collection activities. Whether FISS directed, or motivated by modernization, the majority of targeting efforts will emanate/originate from non-governmental entities.

DSS has assessed that certain U.S.-based and foreign entities to represent foreign illicit trade as front companies. Some of these assessments were confirmed by law enforcement and non-proliferation activities. The majority of the confirmations involved technology diversion attempts to a third entity in embargoed nations. Some of these entities were foreign government/defense activities. DSS assesses an increase in law enforcement and non-proliferation activities associated with DSS reporting in 2001.

DSS has identified two trends associated with foreign-owned cleared defense facilities. In several instances, after attaining favorable special security ratings (IAW mitigating security plan), foreign owner will attempt to exploit its position and place foreign workers in restricted space, disregard foreign visitor sign-in logs at the U.S. facility, and request hurried mailings that require export license. Several times foreign-owned U.S. facilities were contacted by foreign subsidiaries of the foreign owner. Two cases involved foreign requests for export-controlled information that may have led to product requests if cleared facility responded and did not report the suspicious contact. DSS assesses that this exploitation by foreign owners will continue.

DSS assesses that the global business environment will continue to provide some degree of cover for foreign government-sponsored targeting of specific technologies and that these activities at foreign-owned U.S. facilities will increase in 2001.

Appendix

Suspicious Indicators and Security Countermeasures for Foreign Collection Activities Directed Against the U.S. Defense Industry

FOREIGN REQUESTS FOR INFORMATION

Foreign requests for U.S. defense industry science and technology (S&T) program information are the most frequently reported method of operation (MO) associated with foreign targeting activity. Requests frequently involve faxing, mailing, e-mailing, or telephoning to individual U.S. persons rather than corporate marketing departments. The requests may involve surveys or questionnaires and are frequently sent over the Internet.

Indicators

- The requester:
  - has an e-mail address in a foreign country.
  - may be associated with an embargoed country.
  - identifies his status as a student or consultant.
  - identifies himself as a "student" seeking empathy because his nation lacks this scientific or technical information.
  - identifies his employer as a foreign government or the work is being done for a foreign government or program.
  - asks about a technology related to a defense-related program, project, or contract.
  - asks questions about defense-related programs using acronyms specific to the program.
  - insinuates that the identity of the third party he works for is "classified".
  - admits he could not get the information elsewhere because it was classified or controlled.
  - advises the recipient to disregard the request if it causes a security problem or if it is for information the recipient cannot provide due to security classification, export controls, and so forth.
  - assures the recipient that export licenses are not required or are not a problem.
- Recipient has never met or does not normally conduct business with the sender.
- Technology requested is classified, International Traffic in Arms Regulation (ITAR)-controlled, is on the Militarily Critical Technologies List, or has both commercial and military applications.
- Requests may be faxed or mailed to an individual vice the company marketing office.
- Requests may exceed generally accepted terms of information.
- Strong suspicions that a competing foreign company employs the "surveyor".

Recommended Security Countermeasures

- Have a technology control plan.
- Have a written company policy on how to respond to requests.
- Brief employees not to respond to suspicious requests.
- Brief employees to report suspicious incidents to the Facility Security Officer.
- Review how much information you have in the open domain.
- Ask foreigner why he wants the information, who he represents, and for what the U.S. information or products will be used.

WEB-BASED REQUESTS FOR INFORMATION

Web-based requests continue to be a significant source of foreign targeting of U.S. DoD technologies. A wealth of once protected information is now retrievable by individuals from around the world. There appears to be a sharp increase in the use of web-based requests by foreign entities as a means to identify potential targets and to facilitate the actual collection of information. Web-based requests provide a simple, low cost, non-threatening, risk-free means of worldwide attempts to acquire U.S. DoD technology. Web-based requests are inconspicuous and can bypass many traditional security safeguards, thus directly reaching the target.

Indicators

- The cleared defense company does not normally conduct business with the foreign requestor.
- The request originates from an embargoed country.
- The request is, in fact, unsolicited or unwarranted.
- Requestor claims to represent an official government agency but avoids proper channels to make the request.
- The initial request is directed at an employee who does not know the sender and is not in the sales or marketing office.
- The requestor is fishing for information.
- Requestor represents unidentified third party.
- The requestor is located in a country with a targeting history directed at U.S. cleared defense industry.
- The requestor appears to be "skirting controls".
- Several similar requests are made over time.

Recommended Security Countermeasures

- Have a technology control plan.
- Incorporate security into web design and advertising.
- Initiate an active monitoring solution of web site.
- Report request to FSO and report to DSS CI for databasing purpose (in several situations, similar requests were received by different U.S. cleared facilities.)

SOLICITATION AND MARKETING OF SERVICES

Consistent with past reporting, individuals, companies and research facilities offer their technical and business services to U.S. research facilities, academic institutions and the cleared defense industry.

Indicators

- Foreign "scientist" seeks employment associated with sensitive defense technologies.
- Offer to provide offshore software support.
- Foreign government- and business-sponsored internships.
- Invitation to cultural exchange, individual-to-individual exchange or ambassador program.
- Offer to act as sales or purchasing agent in foreign country.

Recommended Security Countermeasures

- Have a technology control plan.
- Report names of foreign scientists and engineers whose solicitation concerns classified or controlled research and technology.
- Obtain recommendations and assess risks posed by software support in a foreign land.
- Receive State Department travel briefings before departing on an exchange or ambassador program.

FOREIGN ACQUISITION OF U.S. TECHNOLOGY/COMPANY

Foreign entities try to access sensitive technologies by purchasing U.S. technology or a U.S. company possessing the sensitive technology/product.

Indicators

- Companies of political and military allies are most likely associated with this activity.
- Foreign competitors seek a position in the U.S. company that affords access to technology.
- New employees hired from the foreign parent company or its foreign partners ask to access classified data.
- Foreign parent company attempts to circumvent the security agreement or, even earlier, avoids or otherwise disrupts or hinders the Foreign Ownership, Control or Influence (FOCI) process.
- Foreign parent employees try to make exceptions to the term of the security agreement.
- Statement that license is not necessary.
- Foreign company ask U.S. company to send information or product to another U.S.-based company for transfer overseas; or via FedEx, or UPS to overseas address.

Recommended Security Countermeasures

- Have a technology control plan.
- Request a threat assessment from the program office.
- Scrutinize employees hired at the behest of foreign entity.

- Conduct frequent checks of foreign visits to determine if foreign interests are attempting to circumvent security agreements.
- Provide periodic threat briefings to outside directors and user agencies.
- Ask what U.S. based company does. Ask why company cooperates with a foreign entity. Ask why foreigner wants product express-mailed. Ask export officer if information/product is export-controlled.

FOREIGN VISITS AT U.S. FACILITIES

Foreign visits to cleared U.S. defense contractors can present potential security risks if sound risk management is not practiced.

Indicators

- A Foreign Liaison Officer or embassy official escorting a visitor attempts to conceal official identities during a supposedly commercial visit.
- Hidden agendas as opposed to the stated purpose of the visit.
- Last minute and unannounced persons added to the visiting party.
- "Wandering" visitor who acts offended when confronted.
- Using alternative methods. For example, if a classified visit request is disapproved, the foreign entity may attempt a commercial visit.
- Visitors ask questions during briefing outside the scope of the approved visit hoping to get a courteous or spontaneous response.
- Visitor claims business interest but lacks experience researching and developing this technology.

Recommended Security Countermeasures

- Have a technology control plan.
- Brief foreign collection threat to all employees involved with the foreign visit. Request foreign intelligence service threat assessments.
- Ensure appropriate personnel, both escorts and those meeting with visitors, are briefed on the scope of the visit.
- The number of escorts per visitor group should be adequate to properly control movement and conduct of visitors.

EXHIBITS, CONVENTIONS AND SEMINARS

These functions directly link programs and technologies with knowledgeable personnel. Conventions may provide foreign entities with targeting information to be used later.

Indicators

- Topics at seminars and conventions deal with classified or controlled technologies and/or applications.

- Country or organization sponsoring seminar or conference has tried unsuccessfully to visit the facility.
- Receive invitation to brief or lecture in a foreign country with all expenses paid.
- Requests for presentation summary 6-12 months before seminar.
- Photography and filming appear suspicious.
- Attendees wear false nametags.
- Casual conversation and discussions during and after these events.

Recommended Security Countermeasures

- Have a technology control plan.
- Be aware of follow-up requests after a show.
- Consider what information is being exposed, where, when, and to whom.
- Provide employees with detailed travel briefings concerning the threat, precautions to take, and how to react to elicitation.
- Take mock-up displays instead of real equipment.
- Request a threat assessment from program office.
- Restrict information provided to that necessary for travel and hotel accommodations.
- Carefully consider whether equipment or software can be adequately protected.

EXPLOITATION OF INTERNET

Internet exploitation consists of hacking, probes, scanning, and pinging. This category is not related to the Internet based requests for information. The majority of cases involve probing efforts. Although probing a system is legal, once a port is breached a crime is committed.

Indicators

- Computer probes are most likely searching for potential weaknesses in systems for exploitation
- Network attacks originated from foreign Internet service providers.
- Attacks last over a period of a day.
- Several hundred attempts are made to use multiple passwords.

Recommended Security Countermeasures

- Have a technology control plan.
- Have firewall monitoring software that logs all intrusion attempts and any malicious activity.
- Have the appropriate level of protection in place to repel such an attack.
- When a probe is noted, heighten security alert status.

JOINT VENTURE/ RESEARCH

Co-production and various exchange agreements potentially offer significant opportunities for foreign interests to target restricted technology.

Indicators

- Resident foreign representative:
  - faxes documents to an embassy or another country in a foreign language.
  - wants to access the local area network (LAN).
  - wants unrestricted access to the facility.
  - singles out company personnel to elicit information outside the scope of the project.
- Enticing U.S. contractors to provide large amounts of technical data as part of the bidding process, only to have the contract canceled.
- Potential technology sharing agreements during the joint venture are one-sided.
- Foreign organization sends more foreign representatives than is necessary for the project.

Recommended Security Countermeasures

- Have a technology control plan.
- Review all documents being faxed or mailed and have someone translate.
- Provide foreign representatives with stand alone computers.
- Share the minimum amount of information appropriate to the scope of the joint venture/research.
- Extensively educate employees on the scope of the project and how to deal with and report elicitation. Periodic sustainment training must follow initial education.
- Refuse to accept unnecessary foreign representatives into the facility.

TARGETING OF U.S. CONTRACTORS ABROAD

Suspicious activity occurs on collector's home territory leaving U.S. travelers vulnerable to exploitation, including that by Foreign Intelligence Services (FIS). Frequently, FIS recognize U.S. travelers who are engaged in international conventions, support to combined military operations, and joint ventures.

Indicators

- Technical means (for example, electronic surveillance).
- Entrapment schemes such as honeytrap, black market and extortion.
- Repeat stays in the same room of the same hotel.
- Several attempts are made to access room by service personnel.
- Excessively helpful assistance.
- Undue questioning by port authorities.

Recommended Security Countermeasures

- Have a technology control plan
- Cleared defense contractors should review the type and amount of information he/she provides and withhold non-essential biographic and other data requested by the host.

WORK OFFERS

Foreign scientists, students, and engineers will offer their services to research facilities, academic institutions, and even cleared defense contractors. This may be a MO to place a foreign national inside the facility to collect information concerning a desired technology.

Indicators

- Foreign applicant has a scientific or engineering background in a technical area for which his/her country has been identified as having a collection requirement.
- Foreign applicant offers services for "free," stating that a foreign government agency, military activity, university, or corporation is paying expenses.
- Foreign intern (students working on masters or doctorate) offers to work without pay under a knowledgeable individual, usually for a period of 2-3 years.
- The technology in which the foreign individual wants to work or conduct research is frequently related to, or may be classified, ITAR , MCTL or export-controlled.

Recommended Security Countermeasures

- Have a technology control plan.
- Provide employees periodic security awareness briefings about long-term foreign visitors.
- Check backgrounds and references of foreign job, research and intern applicants.
- Request a threat assessment from the program office whose goals are associated with the foreign interest.

CO-OPTING FORMER EMPLOYEES

Former employees who had access to sensitive, proprietary, or classified S&T program information remain a potential counterintelligence concern. Targeting cultural commonalties to establish rapport is often associated with this collection attempt. Former employees may be viewed as excellent prospects for collection operations and considered less likely to feel obliged to comply with U.S. Government or corporate security requirements.

Indicators

- Former employee takes a job with a foreign company working on the same technology.
- Former employee maintains contact with former company and employees.
- An employee alternates working with U.S. companies and foreign companies every few years.

Recommended Security Countermeasures

- Have a technology control plan
- Brief employees to be alert to actions of former employees returning to the facility.
- Have a policy concerning visitation or contacts with current employees by former employees.

- Debrief former employees upon termination of employment and reinforce their legal responsibilities to protect classified, proprietary, and export-controlled information.

TARGETING CULTURAL COMMONALITIES

Foreign entities exploit the cultural background of company personnel, visitors and visited, to elicit information.

Indicators

- Employees receive unsolicited greetings or other correspondence from embassy, company, or country of family's origin.
- Employees receive invitations to visit country of family's origin for purpose of providing lecture or receiving an award.
- Foreign visitors single out company personnel of same cultural background with whom to work or socialize.

Recommended Security Countermeasures

- Have a technology control plan.
- Brief all employees on this MO and address it in the company reporting policy.
- Monitor foreign visitor activities for indications of their targeting of company personnel.
- Report suspected targeting as early as possible to minimize potential problems.